有理点を持たない楕円曲線について(代数的整数論 : 最近の種々の話題について)

AUTHOR(S):

中川, 仁; 堀江, 邦明

数理解析研究所講究録
658巻 1988年 129-138

有理点を持たない楕円曲線について

上越教育大　中川　仁　(Jin Nakagawa)
山口大　教養　堀江　邦明 (Kuniaki Horie)

§1. Introduction.

この講演の目的は、「有理数体上定義された楕円曲線で、Mordell-Weil 群が自明であるようなものが無限個存在すること」の新証明を与えることである。この事実は基本的には既知のことである。それは、ここ数年間に発表された文献にあるいくつかの定理の直接の帰結である。実際に、E/Q を類数1の虚2次体の整数環を虚数乗法に持つような楕円曲線とする。Waldspurger の定理によって、原始的2次指標 χ で、$L(1,E\chi)\neq 0$ となるものが無限個存在する。ここで、$E\chi$ は E の χ による twist である。このとき、Coates-Wiles の定理によって、$E\chi(Q)$ は有限群である。さらに、E を適当に選んでおけば虚数乗法の理論によって、$E\chi(Q)_{tor}=0$ となる。したがって、$E\chi(Q)=0$ となる。

我々は、全く異なった方法によって上の事実を証明する。

ディオファンタス方程式 $y^2 = x^3 + a$ $(a \neq 0)$ の有理数解の非存在については、Fueter, Brunner, Mordell, K.-L. Chang 等によって研究されてきた。彼等は、有理数解が存在しないための十分条件を2次体 $Q(\sqrt{a}), Q(\sqrt{-3a})$ の不変量を用いて与えている（Mordell [10]）。それらの中で最も簡単な条件は、Fueter によって与えられた条件である。

D を2次体の判別式になるような整数とし、h(D) をその2次体の類数とする。また、E_D を、方程式 $y^2 = x^3 + D$ で定義される Q 上の楕円曲線とする。このとき、

定理A（Fueter, 1930） $D < 0$, $D \equiv 8$ or $12 \bmod 16$, $D \equiv 2 \bmod 9$ かつ $3 \nmid h(D)$ ならば、$E_D(Q) = 0$.

したがって、このような条件を満たす D が無限個存在することがいえればよい。これに関して、次の結果が知られている。

定理B（Hartung, 1974） 任意の素数 p に対して、$p \nmid h(D)$ となる $D < 0$ が無限個存在する。

岩沢健吉氏は1970年の大阪大における講演の中で、上の二つの結果を紹介し、「定理B を合同条件を付けた形に拡張できれば、原点∞以外の有理点を持たない楕円曲線の無限存在の証明を得られる」と指摘した。我々はこの方針に従う。定理B は Kronecker の類数関係式を用いて証明されるが, その証

明を改良して合同条件を付けることは非常に難しいと思われる（Horie [9] を参照）。しかし、幸いなことにp = 3 に対してだけは次の非常に強い定量的な結果が知られている。

定理C (Davenport-Heilbronn, 1971)　$h_3(D)$ によって、2次体$Q(\sqrt{D})$のイデアル類cで $c^3 = 1$ となるものの個数を表す。このとき、

$$\sum_{-X<D<0} h_3(D) \sim 2 \sum_{-X<D<0} 1 \qquad (X \to \infty),$$

$$\sum_{0<D<X} h_3(D) \sim (4/3) \sum_{0<D<X} 1 \qquad (X \to \infty).$$

特に、

$$\liminf_{X\to\infty} \frac{\#\{D; -X<D<0, 3 \nmid h(D)\}}{\#\{D; -X<D<0\}} \geqq \frac{1}{2},$$

$$\liminf_{X\to\infty} \frac{\#\{D; 0<D<X, 3 \nmid h(D)\}}{\#\{D; 0<D<X\}} \geqq \frac{5}{6}.$$

これは2元3次形式の類数に関するDavenportの結果を用いて証明される。我々は定理Cを判別式に任意の合同条件を付けた形に拡張して、次の結果を得た。

定理1　m,N を次の条件（＊）を満たす自然数とする。

（＊）　m,N が奇素数pを公約数に持てば、$p^2 \mid N$, $p^2 \nmid m$.

N が偶数ならば、(i) $4 \mid N$, $m \equiv 1 \bmod 4$ または、

(ii) $16 \mid N$, $m \equiv 8$ or $12 \bmod 16$.

このとき、定理Cにおいて判別式Dにすべて合同条件 $D \equiv m$

mod N を付けた主張は正しい。

定理1と後述の命題1から直ちに次を得る。

定理2

$$\liminf_{X\to\infty} \frac{\#\{D;\ -X<D<0,\ E_D(\mathbb{Q})=0\}}{X} \geqq \frac{1}{16\pi^2}.$$

特に、方程式 $y^2 = x^3 + D$ で定義されるQ上の楕円曲線で原点∞以外には有理点をもたないものが無限個存在する。

定理1にはもう一つ別の応用がある。有限次代数体Kと素数pに対して、$\lambda_p(K)$ をKのbasic Z_p-extensionの岩沢λ不変量とする。Z_p-extensionの理論においてよく知られているように、pのKにおける素因子が唯一かつKの類数がpと素ならば、$\lambda_p(K)=0$ である。特に、$D\equiv 0$ or $2 \bmod 3$ ならば、$\lambda_3(\mathbb{Q}(\sqrt{D}))=0$ である。したがって、定理1と後述の命題1から直ちに次を得る。

定理3

$$\liminf_{X\to\infty} \frac{\#\{D;\ -X<D<0,\ \lambda_3(\mathbb{Q}(\sqrt{D}))=0\}}{\#\{D;\ -X<D<0\}} \geqq \frac{5}{16},$$

$$\liminf_{X\to\infty} \frac{\#\{D;\ 0<D<X,\ \lambda_3(\mathbb{Q}(\sqrt{D}))=0\}}{\#\{D;\ 0<D<X\}} \geqq \frac{25}{48}.$$

§2. 定理1の証明

まず、Davenport-Heilbronnの証明の主なアイディアを復習する。K/Qを3次体とし、D_K をKの判別式とする。Kの

整数環O_Kの基底$1,\omega,\nu$をとり、

$f_K(x,y)=\Delta^{1/2}(x\omega+y\nu)/D_K^{1/2}$とおく。ここで、$\Delta(\alpha)$はKの元$\alpha$の判別式を表す。$f_K(x,y)$は整数係数2元3次形式であり、原始的（係数の最大公約数が1）、Q上既約かつf_Kの判別式$D(f_K)$はKの判別式D_Kに一致することがわかる。もちろん、$f_K(x,y)$は基底$1,\omega,\nu$のとり方によるが、f_KのGL(2,Z)- 同値類$[f_K]$は基底のとり方によらない。そこで、写像

$$\begin{array}{ccc}\{3\text{次体}\} & \to & \{\text{整数係数2元3次形式のGL(2,Z)- 同値類}\} \\ \cup & & \cup \\ K & \longmapsto & [f_K]\end{array}$$

を考える。この写像は単射であり、像も合同条件で決定される。このことから、ある条件を満たす3次体の個数を数えるには、対応する条件を満たす整数係数2元3次形式の同値類の個数を数えればよいことになる。今、非アーベルな3次体K/Qに対して、LをそのQ上のガロア閉包、FをLに含まれる2次体とする。このとき、L/Fが不分岐3次巡回拡大となるための必要十分条件は、$D_K=D_F$となることである。さらに類体論によって、2次体の判別式Dに対して、

$$(h_3(D)-1)/2 = \#\{3\text{次体}\ K/Q;\ D_K=D\} \quad \cdots\cdots(1)$$

が成立する。そこで、整数係数2元3次形式fに対して次の合同条件（**）を考える。

(**) すべての奇素数 p に対して、$D(f) \not\equiv 0 \bmod p^2$,

$$D(f) \equiv 1 \bmod 4 \text{ or } D(f) \equiv 8 \text{ or } 12 \bmod 16.$$

この条件 (**) を満たす整数係数2元3次形式 f 全体の集合を U とする。自然数 N に対して、Z/NZ- 係数の2元3次形式の全体を $\Phi(N)$ とする。このとき、(1) の和をとれば、

$$\sum_{-X<D<0} (h_3(D)-1)/2 = \sum_{-X<D<0} \#\{3\text{次体 } K/Q; D_K = D\}$$

$$\sim \#\{[f]; -X<D(f)<0, (**)\text{を満たす}\}$$

$$\sim \prod_p \frac{\#\{f \bmod q; f \in U\}}{\#\Phi(q)} \#\{[f]; -X<D(f)<0\}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots (2)$$

ここで、(2) の右辺の積はすべての素数 p についての無限積であり、奇素数 p に対しては $q=p^2$, $p=2$ に対しては $q=16$ である。この無限積はリーマンの ζ 関数を用いて、

$$\prod_p (1 - p^{-2})^2 = \zeta(2)^{-2} \qquad \cdots\cdots\cdots\cdots\cdots\cdots (3)$$

と計算される。また、Davenport [3] の結果から、

$$\#\{[f]; -X<D(f)<0\} \sim (\zeta(2)/4)X \qquad \cdots\cdots\cdots\cdots (4)$$

が成立する。さらに、よく知られているように、

$$\sum_{-X<D<0} 1 \sim [2\zeta(2)]^{-1}X \qquad \cdots\cdots\cdots\cdots\cdots\cdots (5)$$

が成立する。したがって、(2) ~ (5) より、

$$\sum_{-X<D<0} h_3(D) \sim \zeta(2)^{-1}X \sim 2\sum_{-X<D<0} 1 \qquad (X \to \infty)$$

を得る。（２）の証明における一つの重要なポイントは、すべての素数pに対する合同条件（**）を満たす２元３次形式fの類を数えることを、合同条件を考えない場合の結果に帰着させることである。したがって、与えられた自然数Nの素因数であるような有限個の素数pの部分だけ合同条件（**）を変更しても、全く同じ議論ができる。これから、定理１を証明するためには次の二つの命題を証明すればよい。

命題１　m,Nを定理１の（*）を満たす自然数とすれば、

$$\sum_{-X<D<0,\, D\equiv m \bmod N} \frac{1}{} \sim \sum_{0<D<X,\, D\equiv m \bmod N} \frac{1}{}$$

$$\sim [\varphi(N)^{-1}\prod_{p\mid N} q(p+1)^{-1}][2\zeta(2)]^{-1}X$$

ここで、φはオイラー関数、q=p（p>2），q=4（p=2）である。

命題２　m,Nを定理１の（*）を満たす自然数とし、

$\Phi(N,m)=\{f\in\Phi(N);D(f)=m\}$ とおけば、

$$\frac{\#\Phi(N,m)}{\#\Phi(N)} = \frac{1}{N}\prod_{p\mid N}\frac{q}{p}(1-p^{-2})$$

ここで、q=p（p>2），q=4（p=2）である。

命題１は解析的整数論においてよく知られた方法で証明される。命題２は$N=p^e$の場合に帰着され、その場合には指数eに関する帰納法で証明される。

§３．超楕円曲線の場合について

Gross-Rohlich は、フェルマー曲線のヤコビ多様体に関する論文[7]の中で、虚２次体の類数に関する次の二つの定理を証明した。

定理D（Gross-Rohlich, 1978） p=5,7 or 11 とすると、有理数 $V \neq 1$, $1-4V^p < 0$ に対して、虚２次体 $Q(\sqrt{1-4V^p})$ の類数は p で割れる。

定理E（Gross-Rohlich, 1978） p を奇素数とすると、自然数 $V > 1$ に対して、虚２次体 $Q(\sqrt{1-4V^p})$ の類数は p で割れる。

そこで、自然数 $n \geq 3$ と虚２次体の判別式 D に対して、$C_{n,D}$ によって方程式 $Dy^2 = 1 - 4x^n$ で定義される Q 上の超楕円曲線（affine 平面曲線とみる）を表すとする。今、n=5,7,11 のいずれかとし、h(D) が n で割れないような D をとる（定理A によって、このような D は無限個存在する）。このとき、定理D によって、$C_{n,D}$ は有理点を持たない。また、n=3 に対しては定理１と Feuter [5] の結果を、n=4 に対しては Aigner[1] と Nagell [11] の結果を用いて、同様の結論がでる。以上をまとめると、

定理４ n が 3,4,5,7,11 のどれかの倍数ならば、$C_{n,D}(Q) = \phi$ となる D が無限個存在する。

整数点についても、定理A と定理E から、次を得る。

定理５　３以上の任意のｎに対して、$C_{n,D}(Z) = \phi$ となるＤが無限個存在する。特に、任意の$g \geqq 1$に対して、種数ｇの超楕円曲線で整数点を持たないものが無限個存在する。

References

1. A.Aigner, Über die Möglichkeit von $x^4+y^4=z^4$ in quadratischen Körpern. Jahresber.d.Deutschen Math. Verein. 43 (1934), 226-229.
2. J.Coates and A.Wiles, On the conjecture of Birch and Swinnerton-Dyer. Invent. math. 39 (1977), 223-251.
3. H.Davenport, On the class-number of binary cubic forms (I). J. London Math. Soc. 26 (1951), 183-192.
4. H.Davenport and H.Heilbronn, On the density of discriminants of cubic fields II. Proc. Royal Soc. London Ser. A 322 (1971), 405-420.
5. R.Fueter, Die Diophantische Gleichung $\xi^3+\eta^3+\zeta^3=0$. Sitzungsberichte Heidelberg Akad. d. Wiss. 25. Abh. (1913), 25pp.
6. R.Fueter, Über kubische diophantische Gleichungen.

Comm. Math. Helv. 2 (1930), 69-89.

7. B.Gross and D.Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. Invent. math. 44 (1978), 201-220.

8. P.Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3. J. Number Theory 6 (1974), 276-278.

9. K.Horie, A note on basic Iwasawa λ-invariants of imaginary quadratic fields. Invent. math. 88 (1987), 31-38.

10. L.J.Mordell, Diophantine equations. New York: Academic Press 1969.

11. T.Nagell, Sur la résolubilite de l'équation $x^2+y^2+z^2=0$ dans un corps quadratique. Acta Arithm. 21 (1972), 35-43.

12. J.L.Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, J. Math. Pures et Appl. 60 (1981), 375-484.